UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,057	08/30/2001	Gregor P. Freund	VIV/0003.01	8336

28653 7590 04/07/2005

JOHN A. SMART
708 BLOSSOM HILL RD., #201
LOS GATOS, CA 95032

EXAMINER	
DIVECHA, KAMAL B	

ART UNIT	PAPER NUMBER
2151	

DATE MAILED: 04/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/944,057	FREUND ET AL.	
	Examiner	Art Unit	
	KAMAL B. DIVECHA	2151	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *THREE* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03/02/2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-64* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-64* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the amendment filed on 03/02/2005. Claims 1-64 are pending in this application.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1,3-6, 8, 11, 12, 17, 21, 45, 46, 47, 48-51, 55 and 57 are rejected under 35 U.S.C. 102(e) as being anticipated by Fuh et al (U.S. Patent No. 6,463,474 B1).

With respect to claim 1, Fuh et al discloses: In a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers (figure 3 item #306, item #210, item #216), a method for managing Internet access based on a specified access policy (see abstract), the method comprising: transmitting a challenge from said client premises equipment to each client computer (figure 4 item #403), for determining whether a given client computer is in compliance with said specified access policy; transmitting a response from at least one client computer back to said client premises equipment, for responding to said challenge that has been issued (figure 4 item #404); and blocking Internet access for any client computer that does not respond appropriately to said challenge (figure 7A block #707).

With respect to claim 3, Fuh et al further discloses the method as in claim 1, wherein a client computer that responds with a particular predefined code indicating non-compliance is blocked from Internet access (figure 7B step #726, #728, #730 and #738).

With respect to claim 4, Fuh et al further discloses the method as in claim 1, wherein a client computer that responds with a particular predefined code indicating compliance is permitted Internet access (figure 7A step #702, #704, #706 and #712).

With respect to claim 5, Fuh et al further discloses the method as in claim 1, further comprising: before receipt of a challenge, transmitting an initial message from a particular client computer to the client premises equipment (figure 4 item #401 sent before #403), for requesting the client premises equipment to transmit a challenge to that particular client computer.

With respect to claim 6, Fuh et al further discloses the method as in claim 5, wherein said initial message comprises a client hello packet (read as a data or http packet or request: figure 4 item #401).

With respect to claim 8, Fuh et al further discloses the method as in claim 1, wherein said access policy specifies rules that govern Internet access by the client computers (column 5 line 67 to column 6 lines 1-5).

With respect to claim 11, Fuh et al further discloses the method as in claim 1, wherein said access policy specifies which applications (read as types of network traffic) are allowed Internet access (column 7 lines 56-58).

With respect to claim 12, Fuh further discloses the method as in claim 1, wherein said access policy (read as user profile) specifies applications (read as types of network traffic) that are allowed Internet access (column 7 lines 56-58).

With respect to claim 17, Fuh et al further discloses the method as in claim 1, wherein said access policy specifies Internet access activities that are permitted or restricted for applications or versions thereof (column 7 lines 56-60; column 5 lines 58-67 to column 6 lines 1-5).

With respect to claim 21, Fuh et al further discloses the method as in claim 1, wherein said challenge includes a request (read as login request) for a particular client computer to respond as to whether it is in compliance with said access policy (figure 4 login request 403 and response 404).

With respect to claim 22, Fuh et al further discloses the method as in claim 1, further comprising: redirecting a client computer that is not in compliance with said access policy to a sandbox server (read as network resource; column 4 lines 62-65); and informing such client computer that it is not in compliance with said access policy (figure 7B step # 730 and 736).

With respect to claim 45, Fuh et al discloses A system for regulating Internet access by client computers (see abstract) comprising: an access policy (read as access privileges) governing Internet access by said client computers (column 6 lines 1-5); client premises equipment serving a routing function (figure 3 item #210) for each client computer to be regulated and capable of issuing a challenge to each client computer (figure 4 a login arrow showed by 403), for determining whether a given client computer is in compliance with said access policy; one or more client computers which can connect to the Internet (column 3 lines 30-35) and at least one of which can respond to challenges issued by said client premises equipment (figure 4 login 403 and response 404); and an enforcement module for selectively blocking Internet access to the

Internet to client computers not in compliance with said access policy (figure 4 block #400 and column 11 lines 30-33).

With respect to claim 46, Fuh et al further discloses the system as in claim 45, wherein said client premises equipment includes a router (figure 3 block #210).

With respect to claim 47, Fuh et al further discloses the system of claim 45, wherein said access policy is provided at each client computer to be regulated (figure 5A item #504 and 506 which are part of access policy for authentication).

With respect to claim 48, Fuh et al further discloses the system of claim 45, wherein said enforcement module is provided at said client premises equipment (figure 4 block #400 in block #210).

With respect to claim 49, Fuh et al further discloses the system of claim 45, wherein said at least one client computer capable of responding to challenges can respond (figure 4 item #404) with a particular predefined code indicating non-compliance (incorrect username and password) with said access policy is blocked from Internet access (figure 7B step #726, #728, #730 and #738).

With respect to claim 50, Fuh et al further discloses the system of claim 45, wherein a client computer that responds with a particular predefined code (figure 4 item #404) indicating compliance (correct username and password) with said access policy is permitted Internet access (figure 7A step #702, #704, #706 and #712).

3. Claim 51 is rejected under the same rationale as claim 5 (see above).

4. Claim 55 is rejected under the same rationale as claim 11 above.

5. With respect to claim 57, Fuh et al further discloses the system of claim 55, wherein said access policy specifies types of activities which applications are allowed to perform or restricted from performing (column 7 lines 55-58).

6. As per claim 9, Fuh et al inherently teaches the process of blocking Internet access includes: determining whether permitting Internet access for a given client computer would violate any of said rules, and if permitting such Internet access would violate any of said rules, denying Internet access for that client computer (fig. 7A and fig. 7B).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

8. Claims 2, 7, 10, 13-16, 18-19, 20, 47, 52-54, 56, 58-60 are rejected under 35 U.S.C. 103(a) as being obvious over Fuh et al (U.S. Patent No. 6,463,474 B1).

Fuh et al discloses all the limitations of claims 1, 5 and 45 as set forth above.

As per claim 2, Fuh et al does not explicitly show a client computer that does not respond at all is blocked from the Internet access, BUT Fuh et al does provide a login page (figure 5A) to client (read as a challenge), wherein if a client does not respond or provide the login information, than the client would be blocked from accessing the network resources, therefore it would have been obvious to the one of ordinary skilled in the art to claim that when a client computer that does not respond at all would be blocked from accessing the network resources because this would have created a secure communication system in a network preventing the resources from hackers and intruders.

As per claim 7, Fuh et al does not explicitly show that the client premises equipment is capable of permitting Internet access by selected client computers and denying access to the other client computers, but Fuh et al does show plurality of users connected to the router (figure 2 item #208a, b and c and item #210) and routers performing the authentication functions wherein if a client fails to provide correct information to the router then a router would block the traffic (figure 7A block #707) to that particular client and when the client provides the correct information, it would be allowed to access the resources (figure 7A block #712).

As per claim 10, Fuh et al does not explicitly show that the access policy includes rules that are enforced against selected ones of users, computers, and groups thereof, but it would have been obvious to the one of ordinary skilled in the art to enforce the rules in the access policy against selected ones of users, computers and groups in order to avoid any unnecessary incoming or outgoing traffic to the network.

As per claims 13-16, Fuh et al does not explicitly disclose: application are specified by executable name and version number, application are specified by digital signatures, digital signatures are computed using a cryptographic hash and wherein said cryptographic hash comprises a selected one of Secure Hash Algorithm (SHA-1) and MD5 cryptographic hashes, however it would have been obvious to the one of ordinary skill in the art to use the above specified elements because it would have allowed a router to make a correct decision (block or permit) by comparing executable names and securely transfer the data to the destination.

As per claims 18 and 19, Fuh et al does not explicitly disclose access policy with rules are transmitted to client computers from a remote location and remote location comprising a centralized location for maintaining said access policy but Fuh et al does show a centralized location where access policy (authentication information and access privileges of users) would have been maintained (figure 3 block #218 and 220) and the link between the client and the centralized location from where the data would have been transferred (figure 3: the communication link 310).

As per claim 20, although Fuh et al does not explicitly teach the method as in claim 1, wherein said blocking step includes: determining, based on identification of a particular client computer or group thereof, a specific subset of rules filtered for that particular client computer or group thereof, but based on the disclosed material by Fuh et al in column 6 lines 1-9 (access privileges), column 8 lines 4-6 (applying appropriate user profile) and figure 7A (based on identification applying filtering mechanism), it would have been obvious to the one of ordinary skill in the art to put this disclosed material together for the benefit of the claimed limitation.

9. Claim 52 is rejected under the same rationale as claim 7 (see above).

10. Claim 53 is rejected under the same rationale as claim 10(see above).

11. Claim 54 is rejected under the same rationale as claim 20(see above).

12. Claim 55 is rejected under the same rationale as claim 11(see above).

13. Claim 56 is rejected under the same rationale as claim 13(see above).

14. Claim 58 is rejected under the same rationale as claim 14(see above).

15. Claim 59 is rejected under the same rationale as claim 15(see above).

16. Claim 60 is rejected under the same rationale as claim 16(see above).

17. Claims 22-25, 27-37, 39, 40 and 42-44 are rejected under 35 U.S.C. 103(a) as being obvious over Fuh et al (U.S. Patent No. 6,463,474 B1) in view of Logan et al (U.S. Patent No. 5,761,683).

Fuh et al discloses all the limitations of claim 1 as set forth above and informing client computer that is not in compliance with said access policy (figure 7B block #736).

As per claim 22, Fuh et al does not explicitly disclose the process of redirecting a client computer that is not in compliance with said access policy to a sandbox server.

As per claim 23, Fuh et al does not explicitly disclose the process of redirecting a client computer that is not in compliance with a particular access policy to a particular port on the sandbox server; and displaying particular error message pages on the sandbox server in response to communications on particular ports.

As per claim 24, Fuh does not explicitly disclose the process of redirecting a request for Internet access by any client computer that does not respond appropriately to said challenge to a sandbox server.

As per claim 25, Fuh does not explicitly disclose the step of displaying an error message on the sandbox server to any client computer that does not respond appropriately to said challenge.

As per claim 40, Fuh et al does not explicitly disclose the process of redirecting a client computer that is not in compliance with a particular access policy, to a particular port on the sandbox server; and displaying error messages on the sandbox server in response to communications on particular ports.

Logan et al explicitly discloses a network based hypertext display system employing a supervisory computer interconnected with one or more information display units and one or more remote document servers. Logan et al further teaches redirection of a URL request to a remote server (column 19 lines 63-67) and returning appropriate error messages that are displayed to indicate to the user that the access did not succeed (column 7 lines 41-48). Also, when the traffic is redirected to the remote server, it would have been redirected to a particular port on the server that would have been configured to receive the incoming traffic.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to incorporate the teaching of Logan et al as stated above with the method and apparatus that provide network access control of Fuh et al for redirecting a client computer to a server and displaying error messages. One of ordinary skilled in the art would have been motivated because it would have avoided the network congestion at the router by handling error notification and correction at a separate system and improved the overall system efficiency.

18. Claim 26 is rejected under 35 U.S.C 103(a) as being obvious over Fuh et al (U.S. Patent No. 6,463,474 B1) in view of Logan et al (U.S. Patent No. 5,761,683) in further view of Shrader et al (U.S. Patent No. 6,026,440).

Fuh et al and Logan et al disclose all the limitation as in claims 25 and 24 above.

However, Fuh et al and Logan et al does not explicitly disclose that after displaying error messages, permitting said client computer to elect to access the Internet.

Shrader et al explicitly discloses a web server account manager plug-in for monitoring resources. Shrader et al further teaches a server returning an error message (e.g. Unauthorized) to the browser and prompting the user for id and password (read as elect to access the Internet, column 4 lines 56-67).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to incorporate the teaching of Shrader et al as stated above with the system and method of Fuh et al and Logan et al because it would have avoided the network congestion at the router and improved routers performance and would have improved the system efficiency by allowing clients to elect to access the Internet at another location.

19. As per Claim 27, Fuh et al teaches a client that responds with a particular predefined code indicating non-compliance (see above) and Logan et al teaches that a client request is redirected to a network resource (read as server, see above).

20. Claim 41 is rejected under the same rationale as claim 26 above.

21. Claim 28 is rejected under the same rationale as claim 4 (see above).

22. Claim 29 is rejected under the same rationale as claim 5 (see above).

23. Claim 30 is rejected under the same rationale as claim 6 (see above).

24. As per claim 31, Fuh et al discloses a router permitting Internet access by selected client computers (figure 2 and figure 7A) and Logan et al discloses redirecting client computers to a network resource (read as server: column 19 lines 63-65).

25. Claim 32 is rejected under the same rationale as claim 10 (see above).

26. Claim 33 is rejected under the same rationale as claim 11 (see above).

27. Claim 34 is rejected under the same rationale as claim 13 (see above).

28. Claim 35 is rejected under the same rationale as claim 17 (see above).

29. Claim 36 is rejected under the same rationale as claim 18 (see above).

30. Claim 37 is rejected under the same rationale as claim 19 (see above).

31. Claim 38 is rejected under the same rationale as claim 20 (see above).

32. Claim 39 is rejected under the same rationale as claim 21 (see above).

33. Claim 42 is rejected under the same rationale as claim 14 (see above).

34. Claim 43 is rejected under the same rationale as claim 15 (see above).

35. Claim 44 is rejected under the same rationale as claim 16 (see above).

36. Claim 61 is rejected under 35 U.S.C 103 (a) as being obvious over Fuh et al (U.S. Patent No. 6,463,474 B1) in view of Durst, Jr. et al (U.S. Patent No. 6,542,933 B1).

Fuh et al discloses all the limitation of claim 45 as set forth above.

However, Fuh et al does not explicitly disclose a sandbox server to which client computers that are not in compliance with said access policy are redirected.

Durst, Jr. et al explicitly disclose a system and method of using machine-readable or human-readable linkage codes for accessing networked data resources. He further teaches redirecting a client computer from an information server to a content server (read as sandbox server, column 3 lines 19-21 and lines 65-67 and figure 2 block #60)

At the time of invention it would have been obvious to a person of ordinary skill in the art to incorporate Durst, Jr et al's teaching as stated above with the system and method of network access control of Fuh et al because it would have improved the routers performance by redirecting the unauthorized traffic to another server and would have also avoided network congestion at the router.

37. Claims 62-64 are rejected under 35 U.S.C 103 (a) as being obvious over Fuh et al (U.S. Patent No. 6,463,474 B1) in view of Durst, Jr. et al (U.S. Patent No. 6,542,933 B1) and in further view of Shrader et al (U.S. Patent No. 6,026,440).

Fuh et al and Durst, Jr. et al discloses all the limitation as in claims 61 and 45 as set forth above.

However, Fuh et al and Durst, Jr. et al does not disclose the following limitations:

As per claim 62, the sandbox server informs non-compliant client computers that they are not in compliance with said access policy.

Shrader et al explicitly discloses a web server account manager plug-in for monitoring resources. Shrader further teaches as in claim 62, the clients are notified (read as inform) by returning error message such as unauthorized to the browser (column 4 lines 56-67 and figure 3).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to incorporate the teaching of Shrader et al with the system and method of Fuh et al and Durst, Jr. et al because it would have provided client computers to correct the network requests and authenticating again in order to access the Internet after being notified by a particular error.

38. As per claim 63, the client computers are allowed to elect to access the Internet (prompting a user for user id and password) after being informed that they are unauthorized (return error message) or they are not in compliance with access policy (column 4 lines 56-67).

39. As per claim 64, Durst, Jr. et al disclose the information server (read as enforcement module) redirecting the client computers to the content server to retrieve primary content file (column 3 lines 19-21) and Shrader et al teaches a server capable of displaying error messages (column 4 lines 56-66).

Response to Arguments

The examiner withdraws all prior objections.

The applicant has amended claims 9, 20 and 38; therefore the examiner withdraws the 112, 2nd paragraph rejection.

The applicant's arguments on double patenting rejections are persuasive; therefore the examiner withdraws the prior double patenting rejection.

Applicant's arguments on art rejections filed 03/02/2005 have been fully considered but they are not persuasive.

In response to applicants arguments, as per claims 1, 3-6, 8, 11, 12, 17, 21, 45, 46, 47, 48-51, 55 and 57; that the references fail to show certain features of applicant's invention, it is noted

that the features upon which applicant relies (i.e., issue challenges to client devices; router-side security component issues challenges; checking whether client computers are in compliance "with rules of an access policy" before permitting internet access; access policy governing Internet access focuses on the state of the client computer such as requiring particular security software to be installed on the client computers; router challenges issued to client computers requesting information to verify that a particular version of software program is installed on the client computers; grounds for blocking Internet access; applicants arguments, page 17-20) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In response to applicant's argument to claims 13-16 that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the motivation for modifying Fuh was that it would have allowed router to make a decision (permit or block) by comparing executable names and securely transfer the data to the destination.

In response to applicant's argument to claims 2, 7, 10, 13-16, 18-19, 20, 47, 52-54, 56, 58-60; 22-25, 27-37, 39, 40, 42; 26, 41; 61; and 62-64, that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e.,

router-side security module) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO-892.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAMAL B. DIVECHA whose telephone number is 571-272-5863. The examiner can normally be reached on 9.00am-5.30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Zarni Maung can be reached on 571-272-3939. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZARNI MAUNG
SUPERVISORY PATENT EXAMINER